What is claimed is:

1. A method of analyzing security events, comprising:

receiving and processing security events, including grouping the security events into network sessions, each session having an identified source and destination;

displaying a graph representing devices in a network, the devices including security devices and non-security devices, the displayed graph including a plurality of individual device symbols and a plurality of group device symbols, each individual device symbol representing a security device of the network and each group device symbol representing a group of non-security devices of the network; and

displaying in conjunction with the graph security incident information, including with respect to a group device symbol an incident volume indicator that indicates a number of network sessions whose source or destination is at any member of a group of non-security devices corresponding to the group device symbol.

2. The method of claim 1, including

upon user selection of a group device symbol for a group of non-security devices, displaying a second level graph representing the non-security devices in the group and the security devices in association with the group, the displayed second level graph including a plurality of non-security device symbols and a plurality of security device symbols, each non-security device symbol representing one non-security device in the group and each security device symbol representing one security device in the group; and

displaying in conjunction with the second level graph security incident information, including with respect to a non-security device symbol an incident volume indicator that indicates a number of network sessions whose source or destination is at the non-security device.

3. The method of claim 1, including

upon user command with respect to a user specified device symbol in the displayed graph, displaying data representing network sessions whose source or destination is at a device corresponding to the user specified device symbol.

4. The method of claim 3, including in response to one or more user commands, selecting a network session from the displayed data, and defining a drop rule that comprises a set of network conditions corresponding to the selected network session;

wherein the processing of security events includes filtering out network sessions that satisfy the defined drop rule.

5. The method of claim 3, wherein the data representing network sessions includes source and destination identifying information, event type information indicating one or more types of incidents corresponding to the network sessions, and security device information indicating one or more security devices that report security events in association with the network sessions.

6. The method of claim 1, wherein the processing of security events includes identifying groups of network sessions that together satisfy a security incident identification rule in a group of predefined security incident identification rules, and identifying as rule firing network sessions each of the network sessions that is a member of any identified group of network sessions;

wherein each incident volume indicator indicates a number of rule firing network sessions whose source or destination is at a device corresponding to the device symbol.

7. The method of claim 6, wherein the processing of security events includes excluding from the rule firing network sessions any network session that satisfies any drop rule in a set of drop rules, each drop rule defining a respective set of conditions.

8. A method of defining a rule, the rule identifying instances of a security incident with respect to security events, the method comprising:

providing a table having a plurality of rows, each row defining a class of security events and defining a logical relationship to the class of security events of a subsequent row in the table, if any;

enabling user editing of the table to define one or more constraints in one or more rows of the table, the one or more constraints based upon a group of event parameters comprising a source address, a destination address, and an event type; and

enabling user editing of the table to specify the logical relationship of a user selected row of the table with respect to a subsequent row of the table, the specified logical relationship selected from a predefined set of Boolean relationships and timing relationships.

9. The method of claim 8, wherein the one or more constraints include a constraint that specifies the source address of the class of security events of one row to be the destination address of the class of security events of another row in the table.

10. The method of claim 8, wherein the one or more constraints include a constraint that specifies one or more event types for the class of security events.

11. The method of claim 8, wherein the one or more constraints include a constraint that specifies a number of security events that must satisfy all other constraints specified by a row of the table.

12. The method of claim 8, wherein the one or more constraints include a constraint that specifies a number of security events that must satisfy all other constraints specified by a row of the table in order for the row to be assessed as being satisfied.

13. The method of claim 8, wherein the timing relationship specifies that the class of security events of one row occurs before the class of security events of a subsequent row.

14. A method of defining a query against a plurality of security events to detect a user-defined security event pattern, the method comprising:

collecting a plurality of security events, each event characterized by a set of event parameters including a source address, a destination address, and an event type;

providing a table having a plurality of rows, each row having a plurality of columns and defining a class of security events, one column specifying a logical relationship to the class of security events of a subsequent row in the table, if any, one column specifying a predefined event count of the class of security events;

enabling user editing of the table to define one or more constraints in one or more rows of the table, each of the one or more constraints correlating one or more columns of one row with one or more columns of another row in the table or correlating one or more columns of one row with a predefined set of parameters; and

enabling user editing of the table to specify the logical relationship of a user selected row of the table with respect to a subsequent row of the table, the specified logical relationship selected from a predefined set of Boolean relationships and timing relationships.

15. The method of claim 14, wherein the plurality of rows specify a set of network conditions such that one or more security events that satisfy the set of conditions are skipped from any further processing.

16. A method of analyzing a stream of security events, comprising:

receiving and processing a stream of security events, including grouping the security events into a plurality of network sessions, each session having an identified source and destination and assigned a unique session identifier;

applying a plurality of predefined security event correlation rules to the plurality of network sessions in association with the processed security events;

for each of a subset of the predefined security event correlation rules, identifying network sessions from the plurality of network sessions in association with the processed security events, if any, that satisfy the rule;

displaying a graph representing devices in a network, the displayed graph including a plurality of individual device symbols and a plurality of group device symbols, each individual device symbol representing one security device of the network, and each group device symbol representing a group of non-security devices of the network; and

displaying in conjunction with the graph information associated with the identified network sessions, including with respect to each group device symbol a session volume indicator that indicates a number of identified network sessions whose source or destination is at a non-security device in a group of non-security devices corresponding to the group device symbol.

17. A method of analyzing a stream of security events, comprising:

receiving a stream of security events;

grouping the security events into a plurality of network sessions, each session having at least one security event and characterized by an identified source and destination;

applying a plurality of predefined security event correlation rules to the plurality of network sessions in association with the security events;

for each of a subset of the predefined security event correlation rules, identifying network sessions that satisfy the rule, if any;

displaying a graph representing devices in a network, the displayed graph including a plurality of individual device symbols and a plurality of group device symbols, each

individual device symbol representing a security device of the network, and each group device symbol representing a group of non-security devices of the network; and

displaying in conjunction with the graph information associated with the identified network sessions, including with respect to each group device symbol a session volume indicator that indicates a number of identified network sessions whose source or destination is at a non-security device in a group of non-security devices corresponding to the group device symbol.

18. A network security events analysis system, comprising:

one or more central processing units for executing programs;

an interface for receiving security events; and

a network security event correlation engine executable by the one or more central processing units, the engine comprising:

instructions for receiving and processing security events, including grouping the security events into network sessions, each session having an identified source and destination;

instructions for displaying a graph representing devices in a network, the devices including security devices and non-security devices, the displayed graph including a plurality of individual device symbols and a plurality of group device symbols, each individual device symbol representing a security device of the network and each group device symbol representing a group of non-security devices of the network; and

instructions for displaying in conjunction with the graph security incident information, including with respect to a group device symbol an incident volume indicator that indicates a number of network sessions whose source or destination is at one member of a group of non-security devices corresponding to the group device symbol.

19. The system of claim 18, including

instructions, response to user selection of a group device symbol for a group of non-security devices, for displaying a second level graph representing the non-security devices in the group and the security devices in association with the group, the displayed second level graph including a plurality of non-security device symbols and a plurality of security device symbols, each non-security device symbol representing one non-security device in the group and each security device symbol representing one security device in the group; and

instructions for displaying in conjunction with the second level graph security incident information, including with respect to a non-security device symbol an incident volume indicator that indicates a number of network sessions whose source or destination is at the non-security device.

20. The system of claim 18, including

instructions, responsive to a user command with respect to a user specified device symbol in the displayed graph, for for displaying data representing network sessions whose source or destination is at a device corresponding to the user specified device symbol.

21. The system of claim 20, including instructions, responsive to one or more user commands, for selecting a network session from the displayed data, and defining a drop rule that comprises a set of network conditions corresponding to the selected network session; wherein the processing of security events includes filtering out network sessions that satisfy the defined drop rule.

22. The system of claim 20, wherein the data representing network sessions includes source and destination identifying information, event type information indicating one or more types of incidents corresponding to the network sessions, and security device information indicating one or more security devices that report security events in association with the network sessions.

23. The system of claim 18, wherein the processing of security events includes identifying groups of network sessions that together satisfy a security incident identification rule in a group of predefined security incident identification rules, and identifying as rule firing network sessions each of the network sessions that is a member of any identified group of network sessions; wherein each incident volume indicator indicates a number of rule firing network sessions whose source or destination is at a device corresponding to the device symbol.

24. The system of claim 23, wherein the processing of security events includes excluding from the rule firing network sessions any network session that satisfies any drop rule in a set of drop rules, each drop rule defining a respective set of conditions.

25. A computer program product for use in conjunction with a computer system, the computer program product comprising a computer readable storage medium and a computer program mechanism embedded therein, the computer program mechanism comprising:

instructions for receiving and processing security events, including grouping the security events into network sessions, each session having an identified source and destination;

instructions for displaying a graph representing devices in a network, the devices including security devices and non-security devices, the displayed graph including a plurality of individual device symbols and a plurality of group device symbols, each individual device symbol representing a security device of the network and each group device symbol representing a group of non-security devices of the network; and

instructions for displaying in conjunction with the graph security incident information, including with respect to a group device symbol an incident volume indicator that indicates a number of network sessions whose source or destination is at one member of a group of non-security devices corresponding to the group device symbol.

26. The computer program product of claim 25, including

instructions, responsive to user selection of a group device symbol for a group of non-security devices, for displaying a second level graph representing the non-security devices in the group and the security devices in association with the group, the displayed second level graph including a plurality of non-security device symbols and a plurality of security device symbols, each non-security device symbol representing one non-security device in the group and each security device symbol representing one security device in the group; and

instructions for displaying in conjunction with the second level graph security incident information, including with respect to a non-security device symbol an incident volume indicator that indicates a number of network sessions whose source or destination is at the non-security device.

27. The computer program product of claim 25, including

instructions, responsive to a user command with respect to a user specified device symbol in the displayed graph, for displaying data representing network sessions whose source or destination is at a device corresponding to the user specified device symbol.

28. The computer program product of claim 27, including instructions, responsive to one or more user commands, for selecting a network session from the displayed data, and defining a drop rule that comprises a set of network conditions corresponding to the selected network session; wherein the processing of security events includes filtering out network sessions that satisfy the defined drop rule.

29. The computer program product of claim 27, wherein the data representing network sessions includes source and destination identifying information, event type information indicating one or more types of incidents corresponding to the network sessions, and security device information indicating one or more security devices that report security events in association with the network sessions.

30. The computer program product of claim 25, wherein the processing of security events includes identifying groups of network sessions that together satisfy a security incident identification rule in a group of predefined security incident identification rules, and identifying as rule firing network sessions each of the network sessions that is a member of any identified group of network sessions; wherein each incident volume indicator indicates a number of rule firing network sessions whose source or destination is at a device corresponding to the device symbol.

31. The computer program product of claim 30, wherein the processing of security events includes excluding from the rule firing network sessions any network session that satisfies any drop rule in a set of drop rules, each drop rule defining a respective set of conditions.